Opera Root Program Update

CA/Browser Forum
Shanghai F2F meeting
October 17, 2018

Opera

whoami: Tomasz Nowak

- Desktop Security leader, a member of Opera Security Team

- Recently working on GDPR compliance, Software Assurance process, Bug Bounty program

Opera

About Opera

"Enable global Internet users to discover and access digital content in a fast, easy and personalized manner"

322m MAU
for mobile and PC

- PC browser
- Mobile browsers
- AI-powered personalized news

Opera

Corporate update

- ASA -> AS

- Demerge

- Current owners

- Nasdaq: OPRA (listed in July 2018)

Opera

Our current Root CA Program (certs.opera.com)

Overview

- Opera Desktop:
  - from OS + CRLSets from Chrome
- Opera for Android:
  - from OS + CRLSets from Chrome
- Opera Mini:
  - AndroidCAStore
  - our own (in Turbo mode)
- We also support VEWD (former Opera TV) - 200 mln of devices (TV boxes)
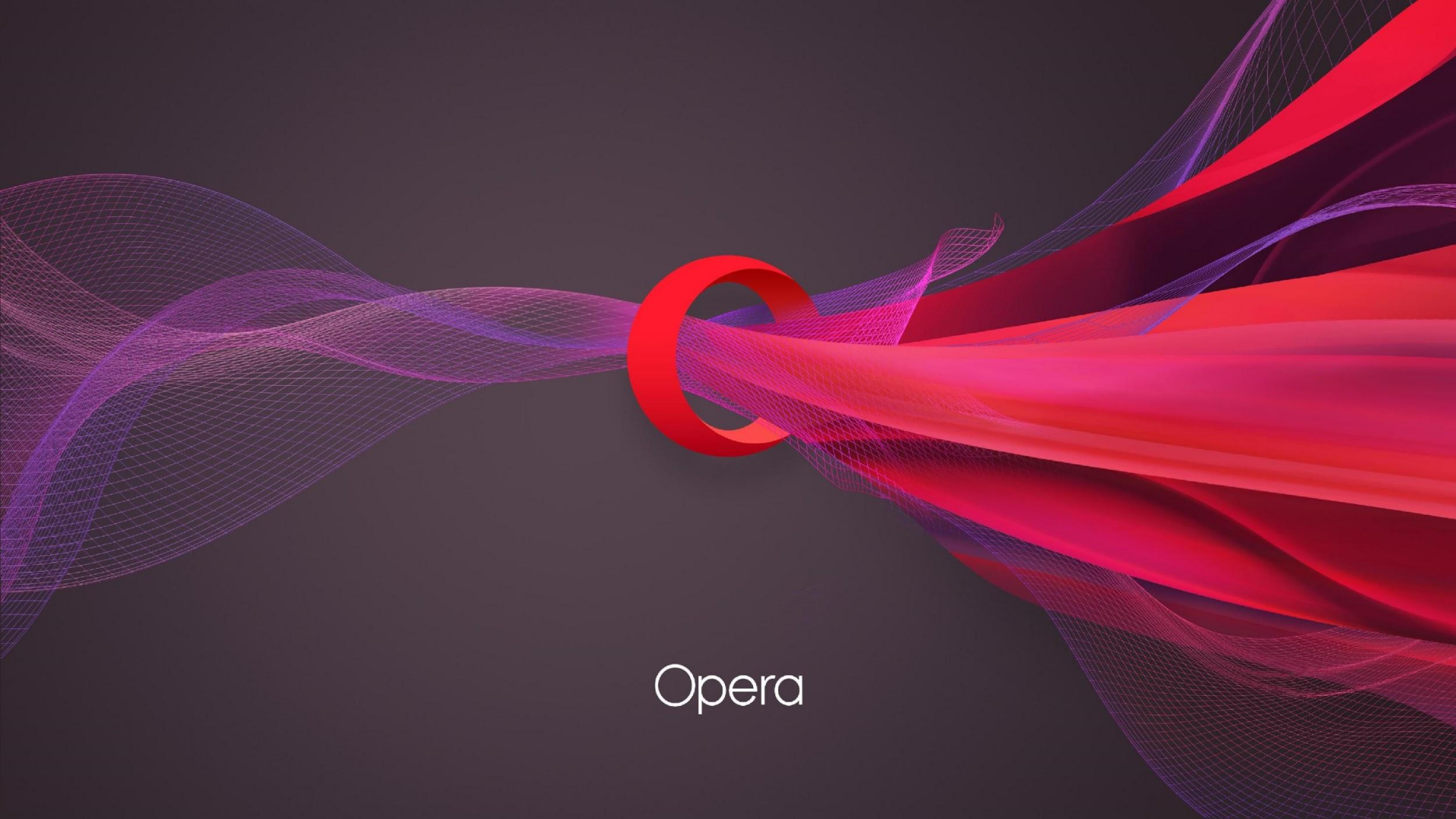
Opera

Quick Facts

- Certificate root store management for Presto-based products (Mini, TV, etc.)
- Basic mechanism:
  - Fetch Mozilla's store
  - Apply our own modifications
  - Sign
  - Serve on certs.opera.com
- No strict update schedule. Update requests usually come from the Mini team.

Opera

Additional blacklist for Desktop

Opera

Additional blacklist for Desktop

- Opera's private certificate revocation list
- Based on CRLSets
- Last updated in 2015-11
- Removed from codebase this month (not to rewrite it to Network Service)
- We believe that lists composed by Operating System Vendors and Google's CRLSets will be updated quick enough

Opera

Opera